
psych ! (つ ■-■)つ
Hacking 101

What we have explored so far...

DAY 1
visualize data tracking + familiarize yourself with coding

DAY 2
dig deeper into media consent + arrays and strings primer

DAY 3
dynamics of censorship + loops and a coding challenge

DAY 4
encryption and encodings + design your own encoding!

DAY 5
Understanding how the internet works + using ESPs

DAY 6
Elaborating on encryption + network using ESPs

DAY 7
Hacking (ethically) + Reflections

Recall !!

behaviour profiling

media tracking

third party websites

cookies

data brokers

IRL examples

censorship

stakeholders

anonymity

content moderation

topology

networks

internet

routers

transmission

Vigenere Solution

- Key (K) : FRINGE
- Plain text(P): get all soldier a meal.
- Cipher text(C):

Note: This Vigenere is P[i] + K[i] + 1

K	F	R	I	N	G	E	F	R	I	N	G	E	F	R	I	N	G	E
P	g	e	t	a	l	l	s	o	l	d	i	e	r	a	m	e	a	l
C	M	W	C	O	S	Q	Y	G	U	R	P	J	X	S	V	S	H	Q

F S Y

Vigenere encryption is where we encrypt on the basis of a keyword. We apply the shift for the plaintext on the basis of the letter of the keyword that corresponds to it.

Vigenere Solution

```
def VigenereDist(word_key, text):

    text = text.upper().replace(" ", "")
    word_key=word_key.upper()

    dict_alpha_initial= {'A' : 0, 'B': 0, 'C': 0, 'D': 0, 'E': 0, 'F': 0, 'G':0, 'H':0, 'I':0, 'J':0, 'K':0, '
    dict_alpha_final= {'A' : 0, 'B': 0, 'C': 0, 'D': 0, 'E': 0, 'F': 0, 'G':0, 'H':0, 'I':0, 'J':0, 'K':0, 'L'

    ciphertext=""
    for i in range(len(text)):
        if text[i].isalpha():
            base_val=65

            cipher_index = ((ord(text[i]) - base_val + ord(word_key[i % len(word_key)]) - base_val) % 26)
            cipher_letter = chr(cipher_index + base_val)

            ciphertext+= str (cipher_letter)
        ------------------------------------
```

Hacking techniques

phishing

Phishing is a form of online fraud where attackers impersonate legitimate organizations or individuals to deceive victims into providing sensitive information. This can include login credentials, financial information, or personal data.

using “baits”

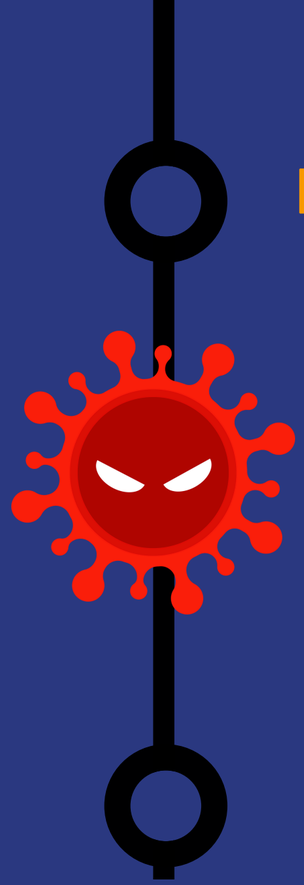
The term "phishing" is derived from "fishing," as attackers use bait (like fake emails or websites) to lure victims.

password hacking

harvesting = Collecting passwords from sources like breaches, phishing, or keyloggers.

spraying = Trying a few common passwords across many accounts to avoid lockouts

credential stuffing = Attacker takes real usernames and passwords (usually leaked from one website) and tries them on other websites.

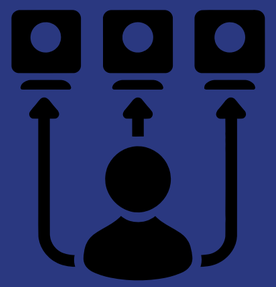


malware deployment

Malicious software used by attackers to gain unauthorized access, steal data, or damage systems. It can be delivered through infected email attachments, malicious links, USB drives, or compromised software.

Once deployed, malware like trojans, ransomware, or keyloggers can silently collect information, encrypt files for ransom, or provide backdoor access for continued exploitation.

Man in the middle (MitM attacks)



A Man-in-the-Middle attack occurs when an attacker secretly intercepts and possibly alters communication between two parties without their knowledge.

This can happen on unsecured networks (like public Wi-Fi), allowing the attacker to eavesdrop on sensitive data such as login credentials, personal information, or financial details.

Types of hackers

white hat hackers

- Work legally to find and fix vulnerabilities
- Often employed as penetration testers or security analysts

grey hat hackers

- Hack without permission but don’t always cause harm
- Often report flaws (sometimes publicly)
- May expect recognition or payment

black hat hackers

- Hack without permission for theft, profit, or damage
- Deploy malware, ransomware, phishing, keyloggers

hactivists

- Hack for political or social causes (e.g., protest)
- Common actions: DDoS, leaks, defacement

Hashing

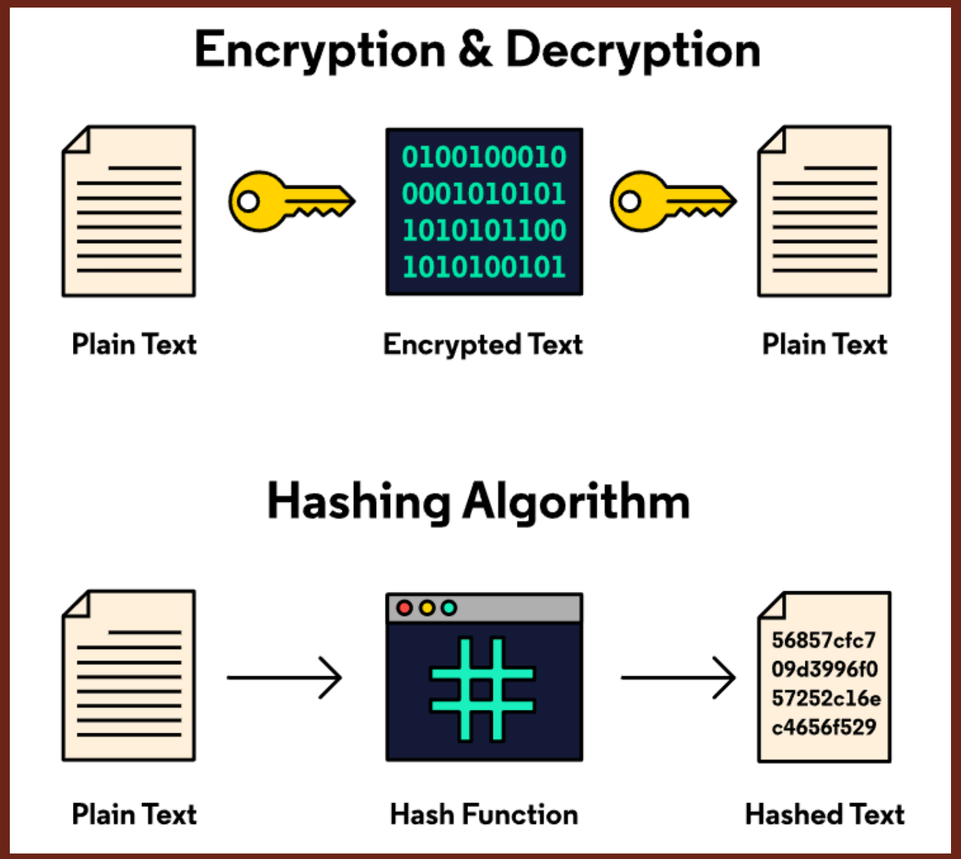
Key features of hashing:

- Deterministic
- Fixed output length
- Pre-image resistance
- Quick Computation

Hashing is the process of converting data – text, numbers, files – into a fixed-length string of letters and numbers. Data is converted into these fixed-length strings, or hash values, by using a special algorithm called a hash function.

For example, a hash function that creates 32-character hash values will always turn text input into a unique 32-character code.

Hashing vs. Encryption



(one way-function)

Hashing	Encryption
one-way process that turns data into a fixed-size string of characters	two-way process that scrambles data so it can only be read by someone with the correct key.
Purpose: securely stores sensitive info. - passwords	Purpose: messages are read only by intended reader

(hashing has avalanche effect: one small change in the inputs can drastically change the hashed out)

e.g. (sha256)
hello:
2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824

Hello:
185f8db32271fe25f561a6fc938b2e264306ec304eda518007d1764826381969

Famous Hacks and how they were achieved

Phishing the employees

↓

Gaining access into control panel

↓

Taking over

Dead Poets Society

Dead, but not dumb!

Context:

You and your friends decided to form a secret club "Dead Poets Society" and hold meetings in a secret room you found in your school. You don’t want your friends or teachers to find out about it, so design a robust cybersecurity system for secured communication and access to the room.

Research and Prepare (15 minutes):

1. Why you need cybersecurity: what are the different ways your communication can be compromised
2. Encryption: how would you encrypt the messages sent across.
3. Key Distribution Protocol: how would you exchange keys among the members.

Presentation (3 mins)

Attacks and Defense (5 mins): Each team attacks once!

You can look up on the internet. If you are found using ChatGPT or other LLMs, you are disqualified. You cannot use the encryption methods or key exchange protocols as they were discussed in class. Either make some tweaks and explain those tweaks or use some other methods and protocols.